UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/630,422	08/01/2000	Leonard Bayer	HAR-002CV	5939

7590 03/15/2006

Kenneth J LuKacher
South Winton Court
3136 Winton Road South Suite 304
Rochester, NY 14623

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 03/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/630,422	BAYER ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27 and 29-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *20-25* is/are allowed.

6)☒ Claim(s) *1-19,26,27 and 29-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The is in response to the applicant's amendment on 27 December 2005.

2. Claims 1-27 and 29-41 are pending in the application.

3. Claims 20-25 have been allowed.

4. Claims 1-19, 26, 27 and 29-41 have been rejected.

Response to Arguments

5. Applicant's arguments with respect to claims 1-19, 26, 27 and 29-41 have been considered but are moot in view of the new ground(s) of rejection.

6. Regarding claims 27 and 29-32, applicant's arguments filed 27 December 2005 have been fully considered but they are not persuasive.

On page 14, the applicant argues that nowhere in Matyas is there an information file encrypted which is sent as part of its survey questionnaires to buyers, but rather the responses to its survey questionnaires are encrypted.

The examiner respectfully disagrees. Matyas discloses encrypting a survey block. The survey block contains multiple surveys. Therefore, since the block is being encrypted then the all surveys contained within are being encrypted.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-3, 12-15, 17-19 and 26 are rejected under 35 U.S.C. 102(e) as being anticipated by Okamoto et al U.S. Patent No. 5,944,794.

As to claim 1, Okamoto et al discloses a system for protecting information received over a network comprising:

at least one first computer system connected to the network [column 8, lines 16-27];

a plurality of second computer systems capable of connecting to the first computer system through the network in which each of the second computers has a user interface to enable the user of the second computer to interact with the first computer system [column 8, lines 16-27];

means for registering one or more of the second computer systems by uniquely identifying each of the second computer systems with the user of the second computer system [column 25, lines 29-61];

means for selecting one or more of the registered second computer systems [column 25, lines 29-61];

means for sending content information from the first computer system via the network to at least one of the selected registered second computer systems without associated information defining the use of the content information by the second computer systems [column 25, lines 29-61];

means for displaying of the received content information at the registered second computer system that receives the content information and limiting the user interface of the second computer system to operate responsive to the user of

the second computer system to prevent copying of the content information when the received content information is being displayed [column 28, lines 5-65].

As to claims 2 and 18, Okamoto et al discloses that the content information sent to one of the registered second computer systems is encrypted, further comprising:

means at the second computer system for requesting a key from the first computer system for decrypting the received encrypted content information [column 25 line 62 to column 26 line 23];

means at the first computer system for sending a key to decrypt the encrypted content information to the second computer system that requested the key [column 25 line 62 to column 26 line 23];

means at the second computer system for decrypting the encrypted content information in accordance with the received key, in which the second computer system when displaying the decrypted content information ignores signals from the user interface capable of enabling access to the decrypted content information [column 25 line 62 to column 26 line 23].

As to claims 3 and 19, Okamoto et al discloses that one more of the registered second computer systems are selected by the selecting means to view the content information. Okamoto et al discloses that the key sending means only sends the keys to the selected second computer systems [column 25 line 62 to column 26 line 23].

As to claim 12, Okamoto et al discloses that the first computer system comprises one or more server computers and a database coupled to at least one of the server computers storing at

least information representing the registered second computer systems and information related to the users of each of the registered second computer systems [column 26, lines 36-48].

As to claim 13, Okamoto et al discloses that the second computer systems each have means for interfacing to the network and capable of connecting to the first computer system at one or more network addresses [column 26, lines 36-48].

As to claim 14, Okamoto et al discloses that the network represents a public network [column 8, lines 42-62].

As to claim 15, Okamoto et al suggests that the content information is part of a survey [column 25 line 62 to column 26 line 23].

As to claim 17, Okamoto et al discloses a method for protecting information received over a network, such as the Internet, comprising the steps of:

at least one first computer system connected to the network [column 25, lines 29-61];

a plurality of second computer systems capable of connecting to the first computer system through the network in which each of the second computers has a user interface to enable the user of the second computer to interact with the first computer system [column 25, lines 29-61];

means for registering one or more of the second computer systems by uniquely identifying each of the second computer systems with the user of the second computer system [column 25, lines 29-61];

selecting one or more of the registered computer systems [column 25, lines 29-61];

means for sending content information from the first computer system to at least one of the selected registered second computer systems without associated information defining the use of the content information by the second computer systems [column 25, lines 29-61];

means for displaying of the received content information at the registered second computer system that receives the content information and limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information when the received content information is being displayed [column 25, lines 29-61].

As to claim 26, Okamoto et al discloses a system for protecting an information file received over a public network from a World Wide Web site by one or more computer systems capable of communicating via the network to the web site, the system comprising:

a web site connected to the network that uniquely registers one or more of the computer systems identifying the computer system to the web site and stores in a database encrypted information files and their associated keys, in which the web site is capable of sending the encrypted information file to registered computer systems, and sending a key to decrypt an encrypted information file to one of the registered second computer system when the second computer system is authorized to receive the key [column 25, lines 29-61];

each of the computer system being capable of connecting to the web site through the Internet and registered with the web site to send a request to the web site for a certain encrypted information file and to receive the encrypted

information file, and then request a key from the web site to decrypt the file, and in response to receiving the key, decrypts the encrypted information file and plays the file through a window on the display of the computer system [column 25, lines 29-61]; and

each of the computer systems having a display and a user interface in which, when the file is played, signals from the user interface at the second computer system are ignored which enable access to the decrypted file, and when another window is selected than the window displaying the decrypted file, disables the playing, of the decrypted file [column 25, lines 29-61].

8. Claims 27 and 29-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Matyas U.S. Patent No. 6,102,287.

As to claim 27, Matyas discloses an Internet web site for supporting concept surveys which are capable of connecting to one or more client computer systems comprising:

one or more computer servers capable of connecting to the Internet in which the client computer system is registered with the web site [column 4 line 61 to column 5 line 11];

a database coupled to one or more of the servers that stores encrypted information files representing parts of one or more surveys and their associated keys [column 13, lines 48-60], in which the web site is capable of sending the encrypted information file to registered client computer systems for carrying out a survey received by the client computer systems [column 16, lines 29-45], and sending a key to decrypt an encrypted information file to one of the registered

second computer system when the second computer system is authorized to receive the key to enable the client computer system to play the information file as part of the survey, in which the survey represents one or more questions answerable by the user of the client computer system [column 28, lines 49-65].

As to claim 29, Matyas discloses that at least one of the computer servers provides downloadable viewer software to client computer systems capable of requesting and receiving the encrypted information file from the web site, and requesting and receiving the key to decrypt the encrypted information file from the web site, and for displaying the decrypted information file in which during the display the operation of the user interface of the client computer system is limited to prevent copying of the decrypted information file [column 19, lines 24-60].

As to claim 30, Matyas discloses a system for conducting a survey over a network comprising:

at least one first computer system connected to the network [column 4 line 61 to column 5 line 11];

a plurality of second computer systems capable of connecting to the first computer system through the network in which the second computer systems are registered at the first computer system [column 16, lines 29-45];

means for sending a survey from the first computer system to at least one of the registered second computers [column 16, lines 29-45];

means for downloading an encrypted file from the first computer system to the one of the registered second computer systems in which the encrypted file

is stored at the one of the registered second computer systems for use; in the survey [column 28, lines 49-65];

means at the one of the registered second computer systems for requesting a key from the first computer system to decrypt the encrypted file when the one of the registered second computer systems is associated with a participant preselected to take the survey [column 19, lines 24-60];

means for receiving a key at the one of the registered second computers from the first computer system [column 19, lines 24-60]; and

means at the one of the registered second computer systems for decrypting the encrypted file in accordance with the key and playing the decrypted file as part of the survey at the one of the registered second computer systems, in which the survey represents one or more questions answerable by the user of the client computer system [column 19, lines 24-60].

As to claim 31, Matyas discloses that the network represents the Internet, and the first computer system represents one or more computer servers addressable via the Internet [column 11, lines 25-37].

As to claim 32, Matyas discloses means at the one of the registered second computer systems for sending answers to the survey to the first computer system [column 22, lines 27-48].

As to claim 33, Matyas discloses a system for conducting a survey at a computer connected to the Internet comprising a first computer system representing one or more computer servers, and at least one second computer system capable of connecting to the first computer system through the Internet, and the first computer system has a memory storing at least one

survey and one or more downloadable files, the first computer system having keys for decrypting each of the files when encrypted, in which the files are downloadable and the keys are available from at least one network address, wherein:

> the first computer system sends the survey to the second computer system via the Internet which references a network address to obtain a file for the survey [column 19, lines 24-60]; and
>
> the second computer system has memory and downloads the file from the network address for storage in the memory in which the file is encrypted [column 19, lines 24-60], the second computer system requests a key to decrypt the encrypted file from a network address where the key is available, receives a key when the second computer system is associated with a participant selected to take the survey [column 19, lines 24-60], and decrypts the file in accordance with the key and plays the decrypted file as part of the survey [column 19, lines 24-60].

As to claim 34, Matyas discloses that the second computer system further- comprises a display and plays the decrypted file in a window on the display, and protects the window from being accessed by the user of the second computer system when another window on the display is selected [column 19, lines 24-60].

As to claim 35, Matyas discloses that the second computer system is registered with the first computer system for receiving the survey prior to the second computer system receiving the survey [column 19, lines 24-60].

As to claim 36, Matyas discloses that the first computer system sends the key to the second computer system when the key has been requested during a certain period of time [column 19, lines 24-60].

As to claim 37, Matyas discloses that the first computer system sends the key to the second computer system when the second computer system has not already received the encrypted file a preset number of times [column 19, lines 24-60].

As to claim 38, Matyas discloses that the first computer system sends the key to the computer when a participant has not taken the survey.

As to claim 39, Matyas discloses a system for conducting surveys comprising :

at least one first computer system connected to the network representing one or more computer servers [column 19, lines 24-60];

a plurality of second computer systems capable of connecting to the first computer system through the network [column 19, lines 24-60];

a database registering uniquely the second computer systems and associating each of the registering second computer systems with data describing one or more characteristics of the user of the second computer system [column 19, lines 24-60];

the first computer system enabling selection of one or more users from the database as participants to take a survey having one or more questions and enabling the selected user to answer the questions[column 19, lines 24-60]; and

the first computer system is capable of sending the survey and sending encrypted content information via the network to at least one of the registered

second computer systems associated with a user selected to participate in the survey, in which the second computer system downloads the survey from a first network address associated with the first computer system [column 19, lines 24-60], requests a key from a second network address associated with the first computer system for decrypting the content information, and when the key is received the second computer system utilizes the key to decrypt the content information and then outputs the decrypted content information as part of the survey in which one or more questions of the survey relates to the outputted content information [column 19, lines 24-60].

As to claim 40, Matyas discloses that each of the second computer systems has a user interface which limits the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information while the received content information is being outputted [column 19, lines 24-60].

As to claim 41, Matyas discloses that the one or more characteristics of the user comprises at least one of age or sex of the user [column 19, lines 24-60].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al U.S. Patent No. 5,944,794 as applied to claim 1 above, and further in view of Kim et al U.S. Patent No. 6,584,199 B1.

As to claims 4 and 5, Okamoto et al does not teach that the key sending means only sends the key during a certain time period. Okamoto et al does not teach that the key sending means only send the key to the second computer system a certain number of times.

Kim et al teaches sending keys during certain time periods. Kim et al teaches sending keys to a second computer system a certain number of times [column 6, lines 4-41].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al so that the keys were sent during certain time periods and only a certain number of times.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al by the teaching of Kim et al because sending during certain periods makes it less susceptible for a third party to intercept the keys. By sending the keys a certain amount of times, there would be less available over a network for a third party to intercept [column 2 line 63 to column 3 line 12].

10. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al U.S. Patent No. 5,944,794 as applied to claim 1 above, and further in view of Okamoto et al U.S. Patent No. 6,584,199 B1.

As to claims 6-8, Okamoto et al does not teach that the sending and display enabling means at the second computer systems is provided by viewer software installed at the second computer system. Okamoto et al does not teach that the registering means is enabled when the viewer software is installed. Okamoto et al does not teach that the viewer software is automatically executed in response to executing a program received by the second computer system via the network.

Okamoto et al teaches that sending and display enabling means at the second computer systems is provided by viewer software installed at the second computer system [column 28, lines 38-52]. Okamoto et al teaches that the registering means is enabled when the viewer software is installed [column 29, lines 7-20]. Okamoto et al teaches that the viewer software is automatically executed in response to executing a program received by the second computer system via the network [column 29, lines 45-61].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al so that the sending and display of the content would have been provide by view software such Internet Explorer or Netscape Navigator installed at the second computer. The computer would have been registered when one of the viewing software was installed on the computer. The viewing software would have been automatically executed in response to executing a program received by the second computer system via the network.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al by the teaching of Okamoto et al because it prevents a user from copying a protected image from within and from without his web browser [column 3, lines 19-30].

11. Claims 9-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al U.S. Patent No. 5,944,794 as applied to claim 1 above, and further in view of Adams et al U.S. Patent No. 5,734,380.

As to claims 9-11, Okamoto et al teaches that the second computer systems each have a display [column 9, lines 47-52].

Okamoto et al does not teach that the display enabling means provides for playing the content information is a window on the display. Okamoto et al does not teach that the display enabling means disables playing of the content information in the window when the user of the second computer system selects another window on the display. Okamoto et al does not teach that the display enabling means places a protection image in the window when the playing of the content information in the window is disabled.

Adams et al teaches that the display enabling means provides for playing the content information is a window on the display. Adams et al teaches that the display enabling means disables playing of the content information in the window when the user of the second computer system selects another window on the display. Adams et al teaches that the display enabling means places a protection image in the window when the playing of the content information in the window is disabled [column 7 line 25 to column 8 line 3].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al so that the display enabling means provided for playing the content information is a window on the display. The display enabling means would have disabled playing of the content information in the window when the user of the second computer system selected another window on the display. The display enabling means would have placed a protection image in the window when the playing of the content information in the window was disabled.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al by the teaching of Adams et al because it ensures that the window is protected from being replaced by another display [column 1, lines 36-57].

12. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Okamoto et al U.S. Patent No. 5,944,794 as applied to claim 1 above, and further in view of Hamlin et al U.S. Patent No. 6,477,504 B1.

As to claim 16, Okamoto et al discloses that the first computer system comprises one or more server computers capable of communicating with the plurality of second computer systems via the network. Okamoto et al discloses a database coupled to at least one of the network computers containing at least information defining the registered second computer systems [column 10, lines 3-11]. Okamoto et al discloses that the content information is sent encrypted by the first computer system [column 7, lines 40-57]. Okamoto et al discloses the first computer system has means for sending to the second computer systems a key to decrypt the encrypted file. Okamoto et al discloses that the second computer system has means for decrypting the

encrypted content information in accordance with the key for displaying the decrypted content information, as discussed above.

Okamoto et al does not teach information identifying which of the registered ones of the second computer systems is associated with participants for the survey. Okamoto et al does not teach information determining whether the participants took the survey. Okamoto et al does not teach that the second computer system is associated with one of the participants for the survey not having taken the survey.

Hamlin et al teaches information identifying which of the registered ones of the second computer systems is associated with participants for the survey. Hamlin et al teaches information determining whether the participants took the survey [column 10, lines 54-67]. Hamlin et al teaches that the second computer system is associated with one of the participants for the survey not having taken the survey [column 13, lines 18-34].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al so that there would have been information identifying which of the registered ones of the second computer systems is associated with participants for the survey. There would have been information determining whether the participants took the survey. The second computer system would have been associated with one of the participants for the survey not having taken the survey.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Okamoto et al by the teaching of Hamlin et al because it provides a mechanism and process that decision makers and researchers alike can use to both quickly and economically reach out and understand the behaviors, opinions and attitudes of

consumers and customers in today's competitive and fast moving market place [column 2, lines 44-48].

Allowable Subject Matter

13. Claims 20-25 are allowed.

As to claim 20, prior art does not disclose, suggest or fairly teach sending a survey to the computer via the Internet that references a network address to obtain a file for the survey. Prior art does not disclose, suggest or fairly teach downloading the file from the network address in which the file is encrypted. Prior art does not disclose, suggest or fairly teach requesting a key to decrypt the encrypted file from a network address where the key is available. Prior art does not disclose, suggest or fairly teach receiving a key at the computer when the computer is associated with a participant selected to take the survey. Prior art does not disclose, suggest or fairly teach decrypting the file in accordance with the key and playing the decrypted file as part of the survey.

Any claims not directly addressed are allowed on the virtue of their dependency.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
March 7, 2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

3/9/06